EL575422536US

ket No. CISCO-3095

UNITED STATES PATENT APPLICATION

FOR

PPP DOMAIN NAME AND L2TP TUNNEL SELECTION CONFIGURATION OVERRIDE

INVENTORS:

PURNAM SHETH
ARAVIND SITARAMAN
CHARLES YAGER
GREGORY BURNS

ASSIGNED TO:

CISCO TECHNOLOGY, INC.

PREPARED BY:

D'ALESSANDRO & RITCHIE
P.O. BOX 640640
SAN JOSE, CA 95164-0640
TELEPHONE: (408) 441-1100
FAX: (408) 441-8400

SPECIFICATION

TITLE OF INVENTION

PPP DOMAIN NAME AND L2TP TUNNEL SELECTION CONFIGURATION OVERRIDE

BACKGROUND OF THE INVENTION

Cross Reference to Related Applications

This application is related to the following:

U.S. Patent Application Serial No. 09/488,394, filed January 20, 2000 in the name of inventors Aravind Sitaramin, Aziz Abdul, Bernard Janes, Dennis Cox, John Joyce, Peter Heitman, Shujin Zhang and Rene Tio, entitled "System and Method for Identifying a Subscriber for Connection to a Communication Network", commonly assigned herewith.

U.S. Patent Application Serial No. 09/488,395, filed January 20, 2000 in the name of inventors Aravind Sitaramin, Dennis Cox, John Joyce and Shujin Zhang, entitled "System and Method for Determining Subscriber Information", commonly assigned herewith.

U.S. Patent Application Serial No. ___________, filed November 13, 2000 in the name of inventors Purnam Sheth, Aravind Sitaraman, Charles Yager and Gregory Burns, entitled "PPP/L2TP Domain Name Pre-Authorization", commonly assigned herewith.

Field of the Invention

The present invention relates to the field of data communications. More particularly, the present invention relates to a system and method for static selection of tunnel-based network connections.

The Background Art

A significant concern of the individual private and public domains making up the Internet or any other system incorporating multiple networks is the ability to ensure that only those subscribers who are authorized to access the individual private and public domains within the comprehensive network have the capability to access such networks. Serious security risks are posed by the possibility of unauthorized users having the know-how and capability to invade the individual private and public domains within the network.

In today's networking environment, many privately owned domain sites exist on the Internet that allow access only to those individuals which have been granted the proper authorization. For example, these may include company owned private domains containing confidential information and, as such, the company may grant access only to those employed by the company, or they may be communities of interest (i.e. "pay-sites") that provide information only to those subscribers which subscribe to the privately owned domain. The subscriber who connects to the Internet, typically by means of an Internet Service Provider (ISP) or Telephone Company (Telco), may also possess the capability to

assume the identity of an authorized user. This capability heightens the potential for security violations.

Additionally, it is becoming increasingly more prevalent for individual computer users to have the capability to remotely access privately owned intra networks. Such Virtual Private Networks (VPNs) allow the user to connect with the private intra network of the company from the user's residence by means of the telephone line or other convenient means. The inception of wireless remote connections have even made it possible for users to connect from almost any imaginable locale. The ability to connect remotely to individual private intra networks, once seen as a luxury, has become so commonplace that many working professionals require such access in order to accomplish their everyday job assignments. In many instances, remote users connect to privately owned intra networks through the same means that individuals connect to the Internet, typically Telcos or ISPs. VPNs are cost-effective because users can connect to the Internet locally and tunnel back to connect to corporate resources. This reduces overhead costs associated with traditional remote access methods.

Figure 1 shows a simplified diagram of a computer user connected to a computer network 10 via a host computer 12 linked to an access point 14 which grants authorization to external networks or domains 16, 18 and 20. The potential for a network security violation is posed by the user having the capability through the access point 14 to reach or "Knock on the door" of home gateways 22, 24 and 26.

Still referring to Fig. 1, the user has access to the computer networks through a workstation or host computer 12. The host computer 12 has the capability to connect with the external networks through an access point 14. An access point 14 is essentially an external location capable of permitting authorized users to access external computer networks. Typically, the access point consists of a series of Network Access Servers (NASs) and other related hardware, software and/or firmware. An access point 14 may also include a modem pool (not shown) maintained by a Telephone Company (Telco) or an Internet Service Provider (ISP) which enables its authorized users or subscribers to obtain external network access through the host computer 12 which has the required dial-up connection capability. Those of ordinary skill in the art will recognize that other types of access methods may be provided by a Telcos or ISP such as frame relay, leased lines, ATM (Asynchronous Transfer Mode), ADSL (Asymmetric Digital Subscriber Line) and the like.

Typically, when the user desires to access a specified domain, such as the first privately owned secured domain site 16, the user runs a network logon application program on the host computer 12 which requires the user to input user identification and authorization information as a means of initiating access to the desired network. This information is then directed to the access point 14 where it is verified to ensure that the host user has the required authorization to permit access to the desired network. Once authorization is granted to the user, a connection is established via the access point 14 with the home gateway 22 of the specified first privately owned secure domain site 16. The connection established may be a tunnel-based connection, such as L2TP (Layer Two

Tunneling Protocol) or L2F (Layer Two Forwarding), or an IP-based (Internet Protocol) connection, such as used with ATM or frame relay. The user of the host computer 12, having established such a connection, has the ongoing capability to access the specified domain until the connection is terminated either at the directive of the user or by error in data transmission. The access point 14 will typically have the capability to connect the user to various other privately owned secured domain sites, such as the second private domain site 18 or the public Internet 20. The user of the host computer 12 may use the PPP protocol to connect through the wholesaler networks to another Home Gateway.

Layer 2 Tunneling Protocol (L2TP) is used in many Virtual Private Networks (VPNs). An L2TP access concentrator (LAC) is a device that the client directly connects to and that tunnels Point-to-Point (PPP) frames to the L2TP network server (LNS). The LAC is the initiator of incoming calls and the receiver of outgoing calls. An L2TP network server (LNS) is the Termination point for an L2TP tunnel and the access point where PPP frames are processed and passed to higher layer protocols. The LNS handles the server side of the L2TP protocol. The LNS terminates calls arriving at any of the LAC's PPP interfaces, including asynchronous, synchronous and ISDN. The LNS is the initiator of outgoing calls and the receiver of incoming calls.

Figure 2 is a block diagram that illustrates an L2TP tunnel and how a user typically connects to a privately owned domain site such as a corporate intranet. Using L2TP tunneling, an L2TP access concentrator (LAC) 100 located at the ISP's point of presence (POP) 105 exchanges PPP messages 110 with remote users 115 and

communicates by way of L2TP requests and responses with the customer's L2TP network server (LNS) 120 to set up tunnels 125. The L2TP protocol passes protocol-level packets through the virtual tunnel 125 between end points of a point-to-point connection. Frames from remote users are accepted by the ISP's POP 105, stripped of any linked framing or transparency bytes, encapsulated in L2TP and forwarded over the appropriate tunnel 125. The customer's home gateway 120 accepts these L2TP frames, strips the L2TP encapsulation, and processes the incoming frames for the appropriate interface.

Turning now to Fig. 3 a block diagram that illustrates the use of AAA servers in an L2TP tunneling network is presented. The selection of the L2TP tunnel 200 at the LAC 205 or NAS is typically determined by an authentication, authorization and accounting (AAA) server 210 based upon the structured username (username@domain) in the PPP authentication packet. The AAA 210 looks up a service profile that matches the domain name string. The service profile includes the IP address of the L2TP network server (LNS) 215 and a password for the tunnel 200. Once tunnels are established, the LAC 205 forwards the subscriber's PPP session to the destination LNS 215 through the L2TP tunnel 200. The ISP or enterprise customer 220 receives new PPP sessions and authenticates the sessions using AAA server 225. Authenticated sessions are established on the LNS 215, while sessions that fail authentication are rejected.

Present methods of establishing a tunnel allow an unauthorized user to reach or "Knock on the door" of another Home Gateway 215, merely by changing the domain name provided in the PPP authentication packet to the domain name of the intended

Home Gateway 215. In this scenario, all users having access to access point 205 would have the potential to reach the privately owned secured domain site. For example, a user having a domain name of xxx@corpA.com may change the domain name in the PPP authentication packet to xxx@corpB.com, allowing the user's PPP session to be forwarded to the corpB LNS through the L2TP tunnel assigned to corpB. Allowing such unauthorized access to a Home Gateway 215 subjects the Home Gateway 215 to potential security risks, including denial of service attacks.

Denial-of-service attacks typically focus on making a service unavailable for normal use, which is often accomplished by exhausting a resource limitation on the network or within an operating system or application. When involving specific network server applications, these attacks can focus on acquiring and keeping open all of the available connections supported by that server, effectively locking out valid users of the server or service. For example, a user intending to exploit present day L2TP systems could flood the network with many PPP sessions targeted to a Home Gateway for which the user is not authorized. Although the LNS authentication process would typically prevent an unauthorized user from access to the corporate intranet, the resources devoted to handling the large number of PPP sessions could adversely affect the services available to authorized users.

The currently available solutions to this problem are very limited and do not offer the level of security protection that most companies operating secured and confidential private intra networks demand. Companies have been able to minimize the risk by

setting up internal access points which effectively cause the user/host to dial-in or connect directly with the private intra network without going through an external ISP or Telco. While this direct-connect service allows some measure of security it does so at the expense of increasing the costs associated with maintaining an internal access point and the additional connection costs related to remote users having to potentially incur long distance telephone service charges.

What is needed is a solution that prevents unauthorized PPP sessions from being forwarded to a destination LNS. A further need exists for such a solution that does not alter the original PPP authentication packet.

BRIEF DESCRIPTION OF THE INVENTION

A method for controlling subscriber access in a network capable of establishing connections with multiple services includes receiving a communication from a subscriber using a first communication network coupled to a second communication network, the communication optionally including a domain identifier associated with a service on the second communication network, and authorizing the subscriber to access a service on the second communication network using a virtual circuit. The authorization is based upon a domain configuration override attribute associated with the virtual circuit used to receive the communication from the subscriber. An access server capable of forcing subscribers of a communications system to gain access exclusively to a domain network associated with a virtual circuit includes an authorizer to grant service authorization to the subscribers based upon a virtual circuit used to make a service request, a virtual circuit profile request generator to generate virtual circuit profile requests and a calculator to determine whether the service associated with the virtual circuit matches the service associated with a domain configuration override attribute.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a block diagram of a computer network wherein the host computer has access to multiple domains within the network.

Fig. 2 is a block diagram that illustrates an L2TP tunnel and how a user typically connects to a corporate intranet.

Fig. 3 is a block diagram that illustrates the use of AAA servers in an L2TP tunneling network.

Fig. 4 is a block diagram of a differentiated computer network that has the capability to force subscribers of the system to gain access exclusively to a domain network associated with a virtual circuit in accordance with one embodiment of the present invention.

Fig. 5 is a flow diagram that illustrates a method for static configuration of tunnel-based network connections in accordance with one embodiment of the present invention.

Fig. 6 is a flow diagram that illustrates a method for static configuration of tunnel-based network connections in accordance with one embodiment of the present invention.

Fig. 7 is a flow diagram that illustrates a method for determining the domain name associated with virtual circuit in accordance with one embodiment of the present invention.

Fig. 8 is a flow diagram that illustrates a method for determining the tunnel ID associated with a virtual circuit in accordance with one embodiment of the present invention.

Fig. 9A is a virtual circuit profile table that illustrates tunnel configuration information that may be stored in accordance with one embodiment of the present invention.

Fig. 9B is a table that includes a list of tunnel IDs and associated virtual circuit identifiers in accordance with one embodiment of the present invention.

Fig. 9C is a virtual circuit profile table that illustrates tunnel configuration information that may be stored in accordance with one embodiment of the present invention.

DETAILED DESCRIPTION OF A PREFERRED EMBODIMENT

Those of ordinary skill in the art will realize that the following description of the present invention is illustrative only and not in any way limiting. Other embodiments of the invention will readily suggest themselves to such skilled persons having the benefit of this disclosure.

In accordance with a presently preferred embodiment of the present invention, the components, processes and/or data structures may be implemented using C++ programs running on high performance computers (such as an Enterprise 2000™ server running Sun Solaris™ as its operating system. The Enterprise 2000™ server and Sun Solaris™ operating system are products available from Sun Microsystems, Inc. of Mountain View, California). Different implementations may be used and may include other types of operating systems, computing platforms, computer programs, firmware and/or general purpose machines. In addition, those of ordinary skill in the art will readily recognize that devices of a less general purpose nature, such as hardwired devices, devices relying on FPGA (field programmable gate array) or ASIC (Application Specific Integrated Circuit) technology, or the like, may also be used without departing from the scope and spirit of the inventive concepts disclosed herein.

The authentication, authorization and accounting (AAA) service performs user authentication, user authorization and user accounting functions. It may be a Cisco ACS™ product such as Cisco Secure™, available from Cisco Systems, Inc. of San Jose,

California, or an equivalent product. In accordance with one embodiment of the present invention, the Remote Authentication Dial-In User Service (RADIUS) protocol is used as the communication protocol for carrying AAA information. RADIUS is an Internet standard track protocol for carrying authentication, authorization, accounting and configuration information between devices that desire to authenticate their links and a shared AAA or AAA proxy service. Those of ordinary skill in the art will realize that other authentication protocols such as TACACS+ or DIAMETER can be used as acceptable authentication communications links between the various communications devices that encompass the data communications network and still be within the inventive concepts disclosed herein.

Turning now to Fig. 4, a block diagram that illustrates a communication system 300 in accordance with one embodiment of the present invention is presented. Users connect to public or private domain networks within communication system 300 through host computers 305, 310, 315. The host computers 305, 310, 315 have the capability to connect or link with domain 320. Domain 320 may be a private domain or a public domain, such as the Internet or a private intra network. These links or connections are established via a series of hardware that serve to grant access to specific domains and transport data packets to and from the host computers 305, 310, 315 and domain 320.

The host computers 305, 310, 315 in this particular computer network are connected to a Publicly Switched Telephone Network (PSTN) 325 via a transmission means 330, 335, 340, such as copper wire or cable. Broadcast mechanisms such as

ADSL (Asymmetric Digital Subscriber Line) may be used. Those of ordinary skill in the art will recognize that other types of broadcast mechanisms may be provided by an ISP or Telco such as Ethernet™, frame relay, leased lines, ATM (Asynchronous Transfer Mode) or the like. Access points 345 are located within a wide area network (WAN) 350 and are operated by Telcos or ISPs. The access points 345 house AAA servers 355, Service Selection Gateways (not shown in Fig. 4), L2TP Access Concentrators (LACs) 360, Digital Subscriber Line Aggregation Multiplexers (DSLAMs) 365, 370, 375 or similar devices. The Service Selection Gateway (SSG) is not an integral part of the present invention and therefore a discussion related to their functionality would not benefit the discussion of the present invention. The SSG serves as a gateway between the user and public area domains, such as the Internet.

In order for a user host to gain access to a public domain network, such as the Internet, users must first dial-in or otherwise make a connection with the SSG through a data-receiving interface (not shown in Fig. 5.). As a threshold matter, an authorizer (not shown in Fig. 5) within the LAC serves to authenticate the identity of the user, ensure authorization and ascertain the nature and scope of the public network services that it will provide.

According to one embodiment of the present invention, an access point 345 includes one or more DSLAMs 365, 370, 375 that service the copper loops between the access point 345 and the Customer Premises Equipment (CPE) 305, 310, 315. DSLAMs 365, 370, 375 may link locally or via an inter-central office (CO) link to LAC 360.

Traffic enters and exits the DSLAM chassis through ports, each of which is assigned a port address. A virtual circuit or channel (VC) is a logical circuit created to ensure reliable communication between two network devices. A VC is defined by a Virtual Path Identifier (VPI) / Virtual Channel Identifier (VCI) pair, which is directly tied to a particular DSLAM port used by a particular subscriber.

The LAC 360 is linked to a separate server/memory device 355, herein referred to as an Authentication, Authorization and Accounting (AAA) server 355. The LAC 360 and the AAA server 355 communicate with one-another according to the Remote Access Dial-In User Service (RADIUS) protocol. The specific details of the RADIUS protocol are well known by those of ordinary skill in the art. Moreover, as will be apparent to those of ordinary skill in the art, the RADIUS protocol has limited applicability to the present invention and, therefore a detailed discussion of this protocol is deemed unnecessary. The preferred methods of the present invention described herein are not limited to the use of the RADIUS protocol and other equivalent authentication protocols may be used.

When the LAC 360 receives a PPP authentication request, a virtual circuit profile request generator (not shown in Fig. 4) generates a request packet and a forwarding interface (not shown in Fig. 4) sends a request packet to the AAA server 350. The packet includes the virtual circuit ID 380, 385, 390 associated with the virtual channel used to receive the PPP session. The AAA server 355 receives a request packet from the LAC 360, consults the data bank of virtual circuit profiles contained in its memory and makes

a match based on the virtual circuit ID 380, 385, 390 provided in the request. In order to access the individual profile, a match must be made between the virtual circuit ID 380, 385, 390 in the request packet and the individual profile. If the virtual circuit ID 380, 385, 390 match, and all other requirements are met, the AAA server 350 sends the LAC 360 a virtual circuit profile packet. The virtual circuit profile packet contains all the pertinent information in the port specific virtual circuit profile that enables the LAC 360 to provide the desired service to the user.

The virtual circuit profile packet travels from the AAA server 350 to a second receiving interface (not shown in Fig. 4) within the LAC 360 where the LAC 360 serves to create secure channels to private areas of the network for those users who are authorized to use such sites and, an assessor within the LAC 360 makes a determination as to whether or not the virtual circuit profile for DSLAM port has a tunnel selection configuration override attribute associated with it. A calculator determines whether the service associated with the virtual circuit matches the service associated with the domain configuration override attribute. If a tunnel selection configuration override attribute does not exist in the profile, a connection is opened through the home gate 395 of the requested private domain 320. If a tunnel selection configuration override attribute does exist in the virtual circuit profile for the specified DSLAM port, or if the PPP authentication packet does not include a domain name, a tunnel is established with the LNS 400 associated with the DSLAM port.

In accordance with one embodiment of the present invention, the LAC service and the LNS may be implemented using a Cisco 6400 Universal Access Concentrator, available from Cisco Systems, Inc. of San Jose, California.

Figures 5 and 6 are flow diagrams that illustrate methods by which a LAC or similar device determines information needed to associate a particular virtual circuit with a tunnel ID.

Turning now to Fig. 5, a flow diagram that illustrates a method for static configuration of tunnel-based network connections in accordance with one embodiment of the present invention is presented. According to this embodiment of the present invention, an AAA server maintains a table of domain names indexed by virtual circuit identifiers, and a LAC maintains a table of tunnel IDs indexed by domain names. At 500, a PPP session is received by a LAC or similar device. At 505, an identifier that uniquely describes the virtual circuit used to receive the PPP session (such as a VPI/VCI identifier) is sent to the AAA server. At 510, a domain name that is associated with the unique identifier is received from the AAA server. At 515, a tunnel ID is determined based upon the domain name. The LAC performs a table lookup to obtain the tunnel ID associated with the domain name. At 520, if a tunnel ID has been determined, a tunneling session with the LNS associated with the tunnel ID is established and the PPP session is forwarded to the LNS.

According to another embodiment of the present invention, the information regarding the mapping between virtual circuit ID and tunnel ID is maintained by the LAC or similar device. Figure 6 is a flow diagram that illustrates a method for static configuration of tunnel-based network connections in accordance with one embodiment of the present invention is presented. At 600, a PPP session is received by a LAC or similar device. At 605, a determination is made regarding whether a domain configuration override attribute exists in a virtual circuit profile associated with the DSLAM port used to receive the PPP session. If a domain override attribute exists or if the PPP authentication packet does not include a domain name (610), at 615, the domain is set to the domain indicated in the virtual circuit profile. If a domain override attribute does not exist, the domain is set to the domain used in the PPP authentication packet at 620. The tunnel ID is determined based upon the domain at 625, and the PPP session is forwarded to the LNS at 630.

Figures 7 and 8 are flow diagrams that illustrate methods by which an AAA server or similar device determines information needed to associate a particular virtual circuit with a tunnel ID.

Turning now to Fig. 7, a flow diagram that illustrates a method for determining the domain name associated with a virtual circuit in accordance with one embodiment of the present invention is presented. At 700, a PPP authentication request including a virtual channel ID is received by an AAA server or similar device. At 705, a determination is made regarding whether a domain configuration override attribute exists

in a virtual circuit profile associated with the DSLAM port used to receive the PPP session. If a domain configuration override attribute exists or if the PPP authentication packet does not include a domain name (710), at 715, the domain associated with the virtual channel is returned. If a domain configuration override attribute does not exist, at 720, the PPP domain used in the PPP authentication request is returned.

Turning now to Fig. 8, a flow diagram that illustrates a method for determining the tunnel ID associated with a virtual circuit in accordance with one embodiment of the present invention is presented. At 800, a PPP session including a virtual channel ID is received. At 805, a determination is made regarding whether a domain configuration override attribute exists in a virtual circuit profile associated with the DSLAM port used to receive the PPP session. If a domain configuration override attribute exists, at 815, the tunnel ID associated with the virtual channel is returned. If a domain configuration override attribute does not exist, at 820, the PPP domain used in the PPP authentication request is returned.

Figures 9A-9C are tables that illustrate tunnel configuration information that may be stored in a LAC, an AAA server, or other similar devices in accordance with embodiments of the present invention. Figure 9A is a virtual circuit profile table that contains a list of domain names 900 indexed by virtual circuit IDs 905. A domain configuration override attribute 910 determines whether a subscriber is limited to establishing a tunnel with a particular domain.

Figure 9B is a table that includes a list of tunnel IDs 915 indexed by domain names 920. Table 9B may be used in conjunction with table 9A to obtain a tunnel ID 915 associated with a virtual circuit ID 905.

Figure 9C is a virtual circuit profile table that contains a list of tunnel IDs 925 indexed by virtual circuit IDs 930. A domain configuration override attribute 935 determines whether a subscriber is limited to establishing a tunnel with a particular domain. In the example, a port having a virtual circuit ID of 94/22 (940) may use tunnel ID 2210 (945) exclusively.

The tunnel selection configuration override attribute is requested by the domain owner to be placed in virtual circuit profiles. It allows the service provider the capability to ensure that a PPP session originating from a DSLAM port allocated to a particular domain can connect with only that particular domain, regardless of what domain name is entered in the PPP authentication packet. This provides added security to the owner of the private domain by lessening the likelihood of an unauthorized access to the home gateway of a corporate intranet. The service provider would have the control over which ports are allocated to which domains. The service provider would also have control over which ports have the tunnel selection configuration attribute in their virtual circuit profile and are, thus, limited to one domain and which virtual circuit profiles do not contain the tunnel selection configuration override attribute and are, thus, free to connect to more than one domain.

Although embodiments of the present invention is have been described with respect to virtual circuits in an ATM networking environment, it should be understood that a virtual circuit assigned to a subscriber in system may be defined in any suitable networking environment using any suitable communication technologies and protocols, without deviating from the scope of the present invention.

In accordance with a specific embodiment of the present invention, the components, process steps, and/or data structures are implemented using software. This implementation is not intended to be limiting in any way. Different implementations may be used and may include other types of operating systems, computing platforms, and/or computer programs. In addition, those of ordinary skill in the art will readily recognize that devices of a less general purpose nature, such as hardwired devices, devices relying on FPGA (field programmable gate array) or ASIC (application specific integrated circuit) technology, or the like, may also be used without departing from the scope and spirit of the inventive concepts disclosed herewith.

While embodiments and applications of this invention have been shown and described, it would be apparent to those skilled in the art having the benefit of this disclosure that many more modifications than mentioned above are possible without departing from the inventive concepts herein. The invention, therefore, is not to be restricted except in the spirit of the appended claims.